What is Claimed Is:

1. A security method of controlling access of human beings to a secure item, the method comprising the steps of:

(1) retrieving feature data from an identification object, said retrieved feature data representative of facial features of a first person;

(2) capturing facial features of a second person and generating feature data that is representative of facial features of the second person; and

(3) comparing said retrieved feature data to said applicant feature data to determine security access for the applicant.

2. The method of claim 1, further comprising the steps of:

(4) granting access to the applicant if agreement between said retrieved feature data and said second person feature data is above a threshold; and

(5) denying access to the applicant if agreement between said retrieved feature data and said applicant feature data is below said threshold.

3. The method of claim 1, wherein step (1) comprises the step of reading a magnetic medium to retrieve said retrieved feature data.

4. The method of claim 1, wherein step (1) comprises the step of reading an optical medium to retrieve said retrieved feature data.

5. The method of claim 1, wherein step (1) comprises the step of reading a bar code to retrieve said retrieved feature data.

6. The method of claim 1, wherein step (1) comprises the step of reading a 2-dimensional bar code to retrieve said retrieved feature data.

7. The method of claim 1, wherein step (2) comprises the steps of:

(a) taking a picture of the applicant, and generating image data from said picture;

(b) determining a first separation distance on a face of the applicant using said image data;

(c) determining a second separation distance on said face of the applicant using said image data; and

(d) normalizing said second separation distance relative to said first separation distance resulting in a ratio that is included in said applicant feature data.

8. The method of claim 1,wherien step (2) comprises the steps of:

(a) taking a picture of the applicant, and generating image data from said picture;

(b) determining an eye-to-eye separation on a face of said applicant using said image data;

(c) determining a second separation distance on said face of said applicant using said image data; and

(d) normalizing said second separation distance relative to said eye-to-eye separation resulting in a ratio that is included in said applicant feature data.

9. The method of claim 1,wherien step (2) comprises the steps of:

(a) taking a picture of said applicant, and generating image data from said picture;

(b) determining an eye-to-eye separation on a face of said applicant using said image data;

(c) determining a forehead-to-chin separation on said face of said applicant using said image data; and

(d) normalizing said forehead-to-chin separation relative to said eye-to-eye separation resulting in a ratio that is included in said feature data.

10. The method of claim 1,wherien step (2) comprises the steps of:

(a) taking a picture of said applicant, and generating image data from said picture;

(b) determining an eye-to-eye separation of said applicant using said image data;

(c) determining an ear-to-ear separation on said face of said applicant using said image data; and

(d) normalizing said ear-to-ear separation relative to said eye-to-eye separation resulting in a ratio that is included in said applicant feature data.

11. The method of claim 1, wherein step (2) comprises the steps of:

(a) taking a picture of said applicant; and

(b) determining a separation distance between a first and second feature on a face of the applicant, said applicant feature data representative of said separation distance.

12. The method of claim 11, wherein step (b) comprises the steps of:

(i) locating a first eye and a second eye of the applicant; and

(ii) determining an eye-to-eye separation between said first and second eye.

13. The method of claim 11, further comprising the steps of:

(c) determining a second separation distance between a third feature and a fourth feature on the face of the applicant; and

(d) normalizing said second separation distance relative to said first separation distance.

14. The method of claim 1, wherein step (1) comprises the steps of:

(a) reading said card medium to retrieve an ID code representative of said applicant; and

(b) retrieving said feature data using said ID code.

15. The method of claim 14, wherein step (b) comprises the step of retrieving said feature data from a memory, said feature data cataloged using said ID code.

16. The method of claim 1, further comprising the steps of:

(4) capturing said facial features of the card owner to generate said card feature data; and

(5) writing said card feature data to said card medium prior to step (1).

17. The method of claim 1, wherein step (3) comprises the step of comparing a normalized forehead-to-chin separation of the card owner with a normalized forehead-to-chin separation of the applicant.

18. The method of claim 1, wherein step (3) comprises the step of comparing a normalized nostril-to-nostril separation of the card owner with a normalized nostril-to-nostril separation of the applicant.

19. The method of claim1, wherein step (3) comprises the step of comparing a normalized feature separation of the card owner with a normalized feature separation of the applicant.

20. A method of limiting security access to an authorized card owner, the method comprising the steps of:

(1) reading a medium of an access card to retrieve facial features of the card owner;

(2) taking a picture of an applicant and determining facial features of the applicant using the picture; and

(3) comparing said facial features of the card owner with said facial features of the applicant to determine access of the applicant.

21. The method of claim 20, further comprising the steps of:

(4) granting access to the applicant if there is sufficient agreement between said applicant facial features and said card owner facial features; and

(5) denying access to the applicant if there is there is not sufficient agreement between said applicant facial features and said card owner facial features.

22. A method of determining if an applicant is the owner of an access card for security access purposes, the method comprising the steps of:

(1) reading a bar code on an access card, said bar code having feature data representative of facial features of a card owner;

(2) capturing facial features of an applicant and generating applicant feature data that is representative of said applicant facial features, said step (2) comprising the steps of

(a) taking a picture of the applicant,

(b) determining an eye-to-eye separation of the applicant using said picture, and

(c) determining a second separation distance on a face of the applicant using said picture, and normalizing said second separation distance to said eye-to-eye separation;

(3) comparing said applicant feature data to said card feature data to determine security access, comprising the step of comparing said normalized separation distance of said applicant with a corresponding normalized separation distance of said card owner included in said card feature data.

23. The method of claim 22, wherein said second separation distance is a forehead-to-chin separation.

24. The method of claim 22, wherein said second separation distance is a nostril-to-nostril separation.

25. The method of claim 22, wherein said second separation distance is an ear-to-ear separation.

26. A method of recording facial features of a person in a storage medium, the method comprising the steps of:

(1) taking a picture of the person,

(2) generating feature data representative of facial features of the person; and

(3) writing said feature data to said storage medium.

27. The method of claim 26, wherein step (3) comprises the step of writing said feature data to a magnetic medium on an access card.

28. The method of claim 26, wherein step (3) comprises the step of writing said feature data to an optical storage medium on an access card.

29. The method of claim 26, wherein step (3) comprises the step of writing said feature data to a bar code on an access card.

30. The method of claim 26, wherein step (3) comprises the steps of:

(a) writing an ID code associated with the person to an access card; and

(b) storing said feature data in a memory that is cataloged using said ID code.

31. The method of claim 26, wherein step (2) comprises the step of generating feature data representative of facial features of the person, said feature data including at least one first separation distance between at a first face feature and a second face feature.

32. The method of claim 26, wherein step (2) of generating feature data comprises the steps of:

(a) determining a first separation distance between a first facial feature and a second facial feature using said picture;

(b) determining a second separation distance between a third facial feature and a fourth facial feature using said picture; and

(c) normalizing said second separation distance relative to said first separation distance resulting in a ratio that is included in said feature data.

33. The method of claim 32, wherein step (a) comprises the step of determining an eye-to-eye separation of the person using said picture.

34. The method of claim 32, wherein step (b) comprises the step of determining a forehead-to-chin separation of the person using said picture.

35. The method of claim 32, wherein step (b) comprises the step of determining an ear-to-ear separation of the person using the picture.

36. An system for determining security access of an applicant, comprising:

a medium reader, for reading an access card medium to retrieve card feature data, said card feature data representative of facial features of a card owner;

a feature extractor for taking a picture of said applicant, and generating feature data representative of facial features of said applicant; and

a processor for comparing said card feature data to said applicant feature data to determine security access.

37. The apparatus of claim 36, wherein said medium reader comprises a magnetic reader for reading a magnetic card medium on said access card to retrieve said card feature data.

38. The apparatus of claim 36, wherein said medium reader comprises a bar code reader for reading a bar code medium on said access card to retrieve said card feature data.

39. The apparatus of claim 38, wherein said bar code reader comprises a means for reading a 2 dimensional bar code.

40. The apparatus of claim 36, wherein said feature extractor comprises:

a camera for taking a picture of the applicant; and

a second processor for generating said applicant feature data based on image data that is representative of said picture, said processor determining a separation distance based on a first facial feature and a second facial feature, said applicant feature data including said separation distance.

41. The apparatus of claim 39, further comprising a means for generating said image data from said picture.

42. The apparatus of claim 41, wherein said means for generating said image data comprises a computer scanner.

43. The apparatus of claim 40, wherein said camera is a digital camera, said digital camera generating said image data from said picture.

44. A system for determining security access of an applicant, comprising:

a medium reader, for reading an access card medium to retrieve card feature data, said card feature data representative of facial features of a card owner;

a camera for taking a picture of the applicant, said camera including a means for generating image data representative of said picture; and

a processor coupled to said medium reader and said camera, said processor including computer program code for causing said processor to determine if the applicant is the card owner

using said image data of said applicant and said card feature data, said computer program code comprising,

first program code means for causing said processor to determine an applicant feature separation using said image data, said applicant feature separation representing a distance between a first feature and a second feature on a face of said applicant,

second program code means for causing said processor retrieve a card owner feature separation using said card feature data, said card owner feature separation representing a distance between a first feature and a second feature on a face of said card owner, and

third program code means for causing said processor to compare said card owner feature separation to said applicant feature separation and determine agreement for security access.

45. The system of claim 44, wherein said program code means further comprises:

fourth program code means for causing said processor grant access to the applicant if agreement is above a threshold; and

fifth program code means for causing said processor deny access to the applicant if agreement is below a threshold.

46. The system of claim 44, wherein said medium reader is a bar code reader.

47. The system of claim 44, wherein said card owner feature separation is normalized to an eye-to-eye separation of the card owner, and wherein said first program code means comprises program code means for causing said processor to determine an eye-to-eye separation of the applicant using the image data, and normalize said applicant feature separation relative to said eye-to-eye separation.

48. The system of claim 44, wherein said card owner feature separation is a normalized forehead-to-chin separation of the card owner, and wherein said applicant feature separation is a normalized forehead-to-chin separation of the applicant.

49. The system of claim 44, wherein said card owner feature separation is a normalized nostril-to-nostril separation of the card owner, and wherein said applicant feature separation is a normalized nostril-to-nostril separation of the applicant.

50. The system of claim 46, wherein said card owner feature separation is a normalized ear-to-ear separation of the card owner, and wherein said applicant feature separation is a normalized ear-to-ear separation of the applicant.

51. An access card for use with a security system, said access card comprising a storage medium that stores feature data representative of facial features associated with an owner of the access card.

52. The access card of claim 52, wherein said medium is a bar code.

53. The access card of claim 51, wherein said feature data includes separation distances associated with said facial features of said card owner.